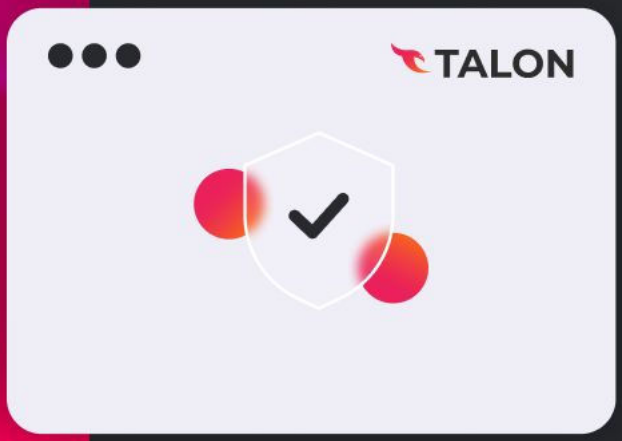
Solution Brief

TalonWork



The browser is where all workers and enterprise assets meet

The way in which companies operate has changed forever: shifting to hybrid work models, increasingly working with third-parties, and moving IT systems to the cloud—including SaaS adoption and a transition to IaaS models. These growing trends have made the browser the optimal hub for hybrid work.

Attackers didn't take long to adapt their techniques to hack current IT stacks, targeting the most-used apps and security blind spots.

Such evolving cyber threats require a change in the way you do security.

The browser is today's #1 most vulnerable application and has a major security blind spot. Offering a new approach, Talon transforms it into your organization's first line of defense. TalonWork not only provides security where it's lacking the most, but also enables enterprise-grade security for workers using any device, anywhere in the world.

The browser – hybrid work's friend or foe?

Today's enterprises rely more on SaaS, flexible working environments, and diverse endpoints. The browser is the one constant within this dynamic reality. Being the most commonly used application, it's the main hub for hybrid work that enables all types of workers to interact with your data and systems. But with the browser's dual role, it's both an enabler and a threat.

Attackers have identified the browser as an opportunity to steal remote information, run malware and exploit it remotely, as well as create malicious extensions they can easily manipulate. Osterman Research says over 60% of malware infecting a given business arrives by way of the browser.

Yet the browser can be used for protection as well. Since it's where users and enterprise assets meet, it's the optimal point to gain visibility and control into all web-based business services—while enhancing a big portion of your present security stack.

TalonWork

Based on Chromium (the open source project behind popular browsers such as Google Chrome and Microsoft Edge), TalonWork provides the browsing experience your team already knows, but with extensive, enterprise-grade security capabilities built-in. It increases visibility, control, and governance—providing your business with the robustness and flexibility required by today's hybrid work environment.

The secure browser

TalonWork is isolated from each device. This protects the browser from compromised endpoints it's running on and reduces its attack surface. With a comprehensive set of embedded security options, and faster, automatic patches, your data and network are protected from malware-infected endpoints, malicious insider activities, and unpatched operating systems.

TalonWork's infrastructure hardening protects against infostealers, man-in-the-browser (MitB) attacks, and malware already installed on a given device. These are known to interact with browsers to steal access tokens, cookies, credentials, or credit cards. TalonWork protects against malicious extensions that can steal data, tokens, or credentials; or can surreptitiously perform actions on behalf users in or outside of your enterprise applications.

TalonWork's anti-tempering capabilities block various techniques commonly used by attackers to manipulate browsers. Bad actors, insiders, and sophisticated workers might use DevTools, malicious JavaScript, remote access, browser debugging, and other anti-tampering and bypass methods to get past enterprise security enforcement policies. TalonWork prevents all of these from occurring.

Physical access protection automatically locks the browser in the event a device is left unattended by a user. Being able to remotely wipe browser data empowers security personnel to immediately revoke access to enterprise services and data whether a user is compromised or their work relationship is subject to an offboarding process.

Zero trust

TalonWork helps secure access to your corporate apps. It can restrict access to your corporate applications only from TalonWork; beyond initial access, it can control restrictions in corporate applications, and also secure corporate data accessed by the managed (or less trusted) device.

TalonWork can:

- Set device posture controls
- Continuously authorize users and devices
- Set granular restrictions for various actions in per corporate app and email domain—such as login, file download/upload/sharing
- Mask data
- Set MFA for login or various actions
- Integrate with an embedded VPN client within the browser

Data Loss Prevention (DLP)

TalonWork provides comprehensive DLP capabilities to prohibit potential data leaks from your enterprise apps. You can configure corporate applications such that data exchange between them is allowed, while leaking data to other applications is blocked.

TalonWork can:

- Control file encryption for files saved on disk
- Set clipboard restrictions between TalonWork and other processes (or between corporate and non-corporate apps)
- Block printing
- Block screenshot

Distributed, Secure Web Gateway (SWG)

TalonWork provides SWG functionality available directly from the browser, including:

- File scanning upon downloading or uploading
- Safe browsing
- URL filtering based on categories, websites or custom domains/URLs
- Network logs for better visibility

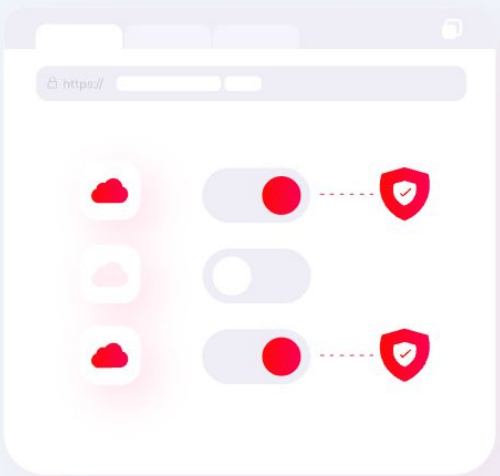
SaaS security

TalonWork provides thorough SaaS monitoring across disparate corporate apps. This includes data auditing across user activities inside SaaS apps, while also supporting on-prem and IaaS apps.
This can assist with:

- Forensics and blue team activities
- Identifying shadow IT
- Letting you know what's happening
- inside your services

Management & control

TalonWork includes a comprehensive SaaS management console. This enables your team to manage all product features, investigate events, perform incident response and forensics, set policies, and manage browser extensions—all within a centralized and intuitive, single-pane console.



Privacy-oriented

TalonWork preserves users' privacy. By being dedicated to work-related web browsing (and potentially separated from a user's personal browser), you're able to monitor all work-related activities without impacting anyone's privacy.

Easy to deploy

Talon delivers all features with a simple deployment. There is no latency and zero infrastructure changes to contend with. Plus, there is no need to redirect traffic or deal with complex SSL-stripping operations.

Use cases

- Secure workspace on non-corporate devices
- Enterprise-grade security across endpoints and SaaS services
- Simple and secure enablement of distributed work models: hybrid work,
  work with third-parties, BYOD
- Additional security layer for highly sensitive business processes
- Accelerated onboarding of new employees and contractors
- Secure and efficient integration of post-M&A subsidiary activities
- Option to supplant existing browser or allow access to corporate apps only from TalonWork

Securing the main hub for hybrid work

TalonWork secures the enterprise work environment by delivering comprehensive security coupled with simple deployment and a frictionless user experience (UX). Enable work from anywhere and BYOD without requiring heavily managed devices or complex and expensive network controls. After a simple one-hour deployment, you'll obtain visibility to the workers' main workspace at the endpoint of every worker—the browser. This is your current frontline and the window to your enterprise assets, so make it secure.